



Trust in the Internet as an experience technology

William H. Dutton & Adrian Shepherd

To cite this article: William H. Dutton & Adrian Shepherd (2006) Trust in the Internet as an experience technology, *Information, Communication & Society*, 9:4, 433-451, DOI: [10.1080/13691180600858606](https://doi.org/10.1080/13691180600858606)

To link to this article: <https://doi.org/10.1080/13691180600858606>



Published online: 20 Nov 2006.



Submit your article to this journal [↗](#)



Article views: 849



Citing articles: 50 View citing articles [↗](#)

William H. Dutton & Adrian Shepherd

TRUST IN THE INTERNET AS AN EXPERIENCE TECHNOLOGY

Trust in the Internet and related information and communication technologies – ‘cybertrust’ – could be critical to the successful development of ‘e-services’, such as e-government, e-commerce, e-learning and democratic participation in the rapidly expanding online public sphere. This paper explores trust in cyberspace based on an analysis of data from an Oxford Internet Survey conducted by the Oxford Internet Institute using a multi-stage, national probability sample in Great Britain. The paper highlights various perspectives on the meaning of trust and draws on findings from the Oxford Internet Survey to explore and refine key social determinants of cybertrust. Evidence from this research provides fresh insights into the factors shaping trust in the Internet, arguing that cybertrust, defined as a confident expectation, is influenced by experience, defined operationally by several indicators of proximity to the Internet, in ways shaped by educational background. The potential for using these results to better understand the role of trust on Internet use is addressed, as well as the more indirect implications for reinforcing digital divides.

Keywords Trust; cybertrust; experience technology; information and communication technologies; social impact; Internet

The social dynamics of cybertrust

The diffusion of the Internet globally and within nations has been rapid since the mid-1990s.¹ Despite reports of many negative online experiences, such as unsolicited junk spam email and viruses, this indicates trust in the Internet remains high enough to maintain its prominent role in communication. However, trust in this new online cyberspace might well shape a person's decision to go online and what is done online, such as whether a person shops or banks electronically, or chats with others (Urban & Sultan 2000).

Some have argued that people who are more trusting in general are more trusting in the Internet (Katz & Rice 2002). For example, a study drawing from US survey data found that individuals who are less trusting of people in general are more likely to perceive the Internet as threatening (Uslaner 2000). In an essay on perceptions of risk in technical and environmental contexts, Douglas and Wildavsky (1982) argue that there are types of individuals with general responses to risks, such as fatalism, shaped by the social and cultural setting in which they are located.

The prominence of 'trust' in discussion of Internet research, practice and policy has not been accompanied by sustained research on how users perceive the Internet. Gaps in the research led us to address the following questions:

- To what extent does the public trust or distrust the Internet's online world?
- Does use of the Internet enhance or undermine trust over time, and with what effect on subsequent patterns of (non-)use?
- How do different social contexts (e.g. generational, educational and geographical) influence issues of trust?
- How does cybertrust shape use of the Internet, for example in relation to different activities such as carrying out financial transactions, looking for medical advice or undertaking scientific research?

The answers to these questions, suggested by the study reported here, were unexpected in a number of ways. Most importantly, experience was the primary factor shaping trust in the Internet – not prior dispositions shaped by a person's age or gender. Also, bad online experiences may have a deterrent effect on using the Internet, as some have feared, but the encountering of bad experiences may not be as great as predicted. This creates a countervailing influence of experience, which generally provides a learned level of trust in the Internet, counterbalanced by exposure to bad experiences, which mitigate perceived benefits.

Defining trust and cybertrust

Trust is a broad concept with application across many disciplines and subject areas, but with no commonly agreed definition. One review of the economic literature on trust found that the existence of uncertainty was one factor present in most definitions of trust (Guerra *et al.* 2003). A conventional usage, as defined by the *Oxford English Dictionary* for example, sees trust as a 'confident expectation': a firm belief in the reliability or truth or strength, etc. of a person or thing and reliance on the truth of a statement, etc. without examination. For example, when someone says they do not trust a story in the newspaper or a post on a Web forum, they might mean that they are uncertain about its truthfulness or they might be certain that it is biased or otherwise misleading.

People therefore seem to define trust to suite their own perceptions and needs, not as economists, sociologists, political scientists or other social scientists might wish to define it, often within experimental settings. However, some general sociological perspectives on attitudes of risk and trust as a reaction to modernity approach the conventional definition used here (e.g. Giddens 1990). It is therefore important to understand the factors that shape trust in cyberspace and why it is useful for survey research on trust to adopt the broad, conventional conceptual definition of a 'confident expectation'. This has been adopted for the study reported here, and operationally defined by responses to particular survey questions.

The substantial effort that has gone into enhancing trust in online products and services such as by devising e-commerce 'trustmarks' (Guerra *et al.* 2003) indicates there is much awareness of the importance of cybertrust. Yet, empirical evidence relating to the social dynamics determining the impact of ICTs on trust is still sparse and contradictory. For instance, some researchers (e.g. Wallace 2001) argue that trust might be undermined in electronic interactions and transactions because the reduced communication channel makes it harder to observe vital non-verbal physical cues, such as facial expressions and body language, that have traditionally been viewed as the prime means used by people to detect deceit. On the other hand, early experiments comparing face-to-face with mediated communication failed to substantiate many conventional expectations about the superiority of face-to-face communication (Short *et al.* 1976). The debate has continued since (see, for example, Ben-Ner & Putterman 2002; Riegelsberger *et al.* 2003), but there is still no definitive research on the impact on perceptions of trust of another person involved in interpersonal communication using different media (face-to-face, audio, visual, Internet, etc.).

Theoretical expectations: the certainty trough

Trust, as conventionally defined, is closely connected with a greater level of certainty or confidence, such as cybertrust in the reliability and security of the Internet. Donald MacKenzie's (1999, pp. 43–46) research posited a 'U-shaped' curvilinear relationship between information and certainty, which he called a 'certainty trough'. At one extreme, those most socially distant from the Internet – with no knowledge of the technology or its use – are likely to be alienated from the technology and least certain about its role. Those who learn more about the Internet, such as by becoming a user, might obtain a higher level of certainty and trust in the technology. At the opposite extreme, ICT professionals, regular Web surfers and others socially closest to the Internet might gain knowledge that increases their level of uncertainty as they learn about complex and difficult-to-manage

issues surrounding online reliability, security and privacy. This suggests that the most informed users and producers of Internet content and services might be less trusting, rather than more.

The degree of such proximity to the technology is just one of many social and institutional factors that could play an important role in determining perceptions of trust.² The research reported here seeks to contribute to the gathering of much needed empirical evidence to provide firmly grounded analyses that offer more reliable insights into how and why Internet users and non-users differ in their patterns of cybertrust. Some recent studies, mainly US based, are also developing such an empirical perspective on trust in the Internet (Lohse *et al.* 2000; Lunn & Suman 2002). Related work is focused on the credibility of specific online content (e.g. Flanigan & Metzger 2000). However, we are not aware of any systematic survey research on cybertrust in the UK prior to the study reported here.

Approach: the Oxford Internet Survey methodology

This paper addresses the cybertrust questions raised above through an analysis of an Oxford Internet Survey (OxIS) study carried out in 2003.³ OxIS is an ongoing, comprehensive investigation of public attitudes in Britain toward the Internet. It includes an examination of levels of trust in various aspects of the Internet, such as opinions regarding the reliability of information on the Web and perceived exposure to a loss of personal privacy and other risks when online.

The study entailed face-to-face interviews with a random sample of people aged 14 and over in England, Wales and Scotland. Personal interviews were conducted through household visits, based on a multi-stage sampling technique designed to provide a sample that could provide projections to the population as a whole.⁴ A probability sample of households was drawn up as the basis for visits. Field staff then randomly sampled individuals within households to determine whom to interview. The aim was to obtain 2000 completed interviews, each lasting around 30 minutes, on a wide range of topics related to the Internet and Web. A high response rate of 66 per cent of those contacted yielded 2030 respondents.⁵ Non-users as well as Internet users were interviewed. Multivariate statistical techniques were used for analysing data from the survey.

Findings: factors shaping key dimensions of cybertrust

The OxIS survey reveals wide variations in cybertrust between individuals. Few respondents exhibit a blind faith in the Internet, but most people are

reasonably confident – if guarded – in the information and people they are able to access over the Internet, but opinions vary widely. For example, when asked how much confidence respondents had in ‘people you can communicate with on the Internet’, 17 per cent of the sample said they had no opinion, while other respondents tended to be distributed across a five-point scale from ‘no confidence’ to ‘total confidence’, with only the latter category representing less than 10 per cent (3 per cent) of all respondents (Dutton & Shepherd 2005, Table 7.2).

Net-confidence and Net-risk

Factor analysis of a set of survey questions related to trust and confidence in the Internet was used to develop indicators that would be more reliable and valid than individual items. Two general categories – two separate dimensions of cybertrust – were defined through a factor analysis. This led us to identify two broad conceptions of trust on the Internet that were empirically defined by the two major factors.

The first was ‘Net-confidence’, the degree to which users and non-users have confidence in the technology and in the people they can communicate with on the Internet. The Net-confidence characteristic of cybertrust was identified primarily through respondents’ answers to three specific questions in the OxIS questionnaire. These related to the extent to which respondents rate: (1) the reliability of information on the Internet; (2) trust the institutions and people ‘running the Internet’; and (3) confidence in the people with whom they interact through this medium.⁶

The second was ‘Net-risk’, the perception of and exposure to risks while using the Internet.⁷ These are distinct, as a person can have very little confidence in the value of information on the Internet but see few risks in its use, or vice versa. The Net-risk dimension of cybertrust was captured by responses to questions about whether Internet users might be exposed to risks, such as losing their privacy, buying the wrong products or not being able to keep personal information secure.⁸

Factors shaping confidence and risk

The ‘certainty trough’ led us to explore trust as a consequence of proximity to the Internet. A relationship emerged between experience and indicators of trust, conceptually defined as a confident expectation. For example, those who do not use the Internet were much more likely to say they did not know whether the information on the Internet was reliable or not; former users express more certainty, but are significantly less certain than are current users (Figure 1). There were similar patterns on the other two issues tied to Net-confidence. For instance, non-users displayed by far the

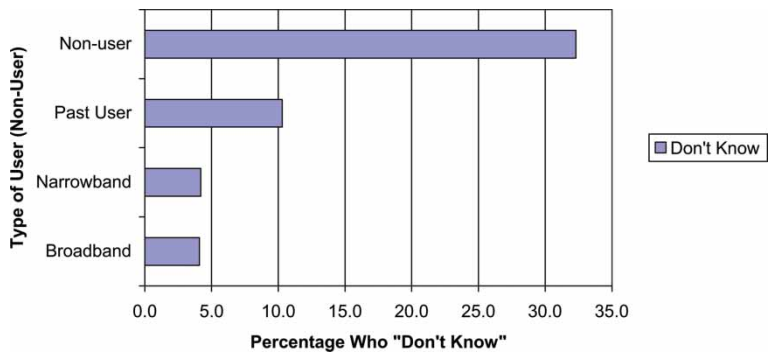


FIGURE 1 A measure of 'Net-confidence': uncertainty over the reliability of information on the Internet ($n = 2029$).

highest degree of uncertainty (about one-third) in the institutions 'running' the Internet and in the people they might encounter online if they were users.

Multivariate analysis of data collected in the survey explored the impacts on cybertrust of a number of factors, in particular users' experience levels and demographic aspects such as gender, age, education and income.⁹ Most generally, use of the Internet is positively associated with the Net-confidence (Table 1) and negatively associated with the Net-risk dimension of cybertrust (Table 2). Experienced users are more confident in the Internet and less concerned over the risks entailed in its use. In addition to use, controlling for other factors, the education of respondents is negatively associated with Net-confidence (Table 1) – being more sceptical of the Internet – but also negatively associated with Net-risk (Table 2) – educated users seeing less risk in using the Internet. Controlling for education and use, other demographic

TABLE 1 Regression coefficients on 'Net-confidence' Scale ($n = 2026$)

variable	<i>B</i> *	<i>std. error</i> *	<i>beta</i> **	<i>t</i>	<i>sig.</i>
constant	−0.34	0.12		−2.78	0.01
gender (female)	0.01	0.06	0.00	0.11	0.91
SES	−0.02	0.02	−0.03	1.20	0.23
age	0.00	0.00	0.02	0.62	0.54
education	−0.04	0.02	−0.05	−2.20	0.03
broadband	0.71	0.08	0.23	8.87	0.00
narrowband	0.71	0.06	0.36	12.78	0.00
past user	0.39	0.10	0.09	4.02	0.00

*Unstandardized coefficients; **Standardized coefficients.

TABLE 2 Multivariate regression coefficients on 'Net-risks' scale (N = 2,026)

<i>variable</i>	<i>B*</i>	<i>std. error*</i>	<i>beta**</i>	<i>t</i>	<i>sig.</i>
constant	0.24	0.13		1.90	0.06
gender (female)	0.11	0.06	0.04	1.76	0.08
SES	-0.03	0.02	-0.04	-1.50	0.14
age	0.00	0.00	0.01	0.44	0.66
education	-0.04	0.02	-0.05	-1.91	0.06
broadband	-0.53	0.08	-0.17	-6.35	0.00
narrowband	-0.16	0.06	-0.08	-2.83	0.00
past user	0.15	0.10	0.04	1.50	0.13

*Unstandardized coefficients; **Standardized coefficients.

factors are not significantly associated with either Net-confidence or Net-risk (Tables 1 and 2).

Among Internet users, we developed a summary scale of their 'proximity' to the Internet based on years of experience, range of uses and expertise. Those users with the highest 'proximity' (more years of experience, a greater range of uses and more expertise) tend to have more Net-confidence, but not in a simple way (Table 3). There is a direct relationship between proximity and Net Confidence but there is also a significant interaction between proximity to the Internet and socioeconomic status. For those in higher socioeconomic groups, proximity to the Internet tends to diminish Net-confidence disproportionately. For those in lower socioeconomic groups, proximity tends to increase Net-confidence. Overall, it appears that proximity tends to undermine predispositions, whether positive or negative, and move all users closer to a learned level of confidence.

TABLE 3 Regression coefficients on 'Net-confidence' for users ($n = 1045$)

<i>variable</i>	<i>B*</i>	<i>std. error*</i>	<i>beta**</i>	<i>t</i>	<i>sig.</i>
constant	0.28	0.15		1.88	0.06
gender (female)	-0.06	0.08	-0.02	-0.78	0.43
SES	0.01	0.03	0.01	0.28	0.78
age	0.00	0.00	0.04	1.40	0.16
education	-0.06	0.02	-0.09	-2.58	0.01
broadband	0.03	0.07	0.01	0.39	0.69
proximity	-0.20	0.10	-0.21	-2.11	0.04
SES*proximity	0.07	0.03	0.27	2.72	0.01
bad net experiences	-0.07	0.03	-0.08	-2.55	0.01

*Unstandardized coefficients; **Standardized coefficients.

While users of the Internet generally exhibit more Net-confidence (see Table 1), they are not blindly trusting. For example, their confidence in the reliability of online information averaged just over six on a 10-point scale, suggesting that they tend to be mindful of the potential for biased information, misinformation or weak sources. Only 3 per cent of all respondents expressed total confidence, suggesting that concerns in the press over meeting ‘strangers’ and ‘bad people’ online have created a healthy scepticism among nearly all users.

The separate Net-risk dimension of cybertrust issues concerns risks to which Internet users might be exposed, such as online fraud, paedophile contacts and an inability to safeguard personal information and privacy. On the one hand, respondents tended to acknowledge that people who go online: put their privacy at risk; enable others to get personal information about them; and make it difficult to judge the quality of a product online. However, as with Net-confidence, individuals vary in their perceptions depending on their experience with the Internet, with users less likely to agree that the Internet puts privacy, personal information or ability to assess products at risk (Figure 2). Non-users exhibit a high degree of uncertainty about Net-risk issues. For instance, almost half of non-users did not know whether the Internet permits people to get personal information about them or if it is difficult to assess product quality online. As one would expect, bad experiences with the Internet tend to increase concerns about Net-risk.

Among users, Net-risk is associated with use of the Internet – experience – and education. Those with a higher level of schooling are likely to be less concerned regarding Net-risks. Those who use broadband Internet and have more proximity to the Internet are also less concerned regarding risks (Table 4).

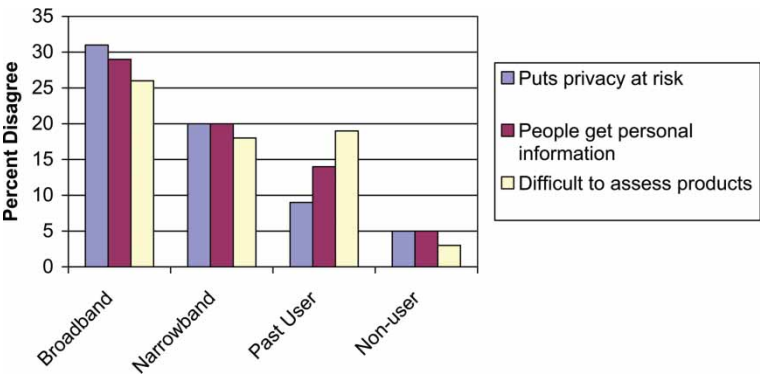


FIGURE 2 Net risks (*n* = 2029).

TABLE 4 Regression coefficients on 'Net-risks' scale for users ($n = 1045$)

<i>variable</i>	<i>B*</i>	<i>std. error*</i>	<i>beta**</i>	<i>t</i>	<i>sig.</i>
constant	-0.09	0.17		-0.53	0.59
gender (female)	0.07	0.09	0.02	0.84	0.40
SES	-0.02	0.03	-0.02	-0.50	0.61
age	0.00	0.00	0.02	0.57	0.57
education	-0.045	0.02	-0.07	-2.16	0.03
broadband	-0.34	0.08	-0.13	-4.20	0.00
proximity	-0.15	0.04	-0.13	-3.89	0.00
bad experiences	0.16	0.03	0.18	5.57	0.00

*Unstandardized coefficients; **Standardized coefficients.

Alternative explanations

Many factors are related to decisions concerning the use and non-use of the Internet. For example, more educated individuals are more likely to use the Internet, and are more trusting. This could indicate that relationships between use and trust are spurious, as they are explained by education. It is therefore important to control statistically for a variety of variables that might explain levels of trust.

Given press attention to inappropriate content for children and to paedophiles attempting to meet children online, one might expect people living in households with children to be more concerned about risks or less confident in the Internet. But in households including at least one person under 18 years of age, we found this variable to be unrelated statistically within any of our models, and experience of the technology diminishes any such concerns.

The Oxis research also found that Internet users in Britain are not more trusting in the Internet simply because they are more trusting of all institutions. Internet users are not significantly more confident in other media than are either non-users or past users. Confidence in the people running newspapers and television is the same for non-users and current Internet users. Internet users are distinctive primarily in the reliability they assign to information on the Internet, which they rate almost as highly as they rate information on television, and higher than they rate newspapers.

Gender, socioeconomic status¹⁰ and age variables were also not significantly related to perceived risks, once other factors are controlled statistically (see Table 3). The most interesting background variable of relevance is education. There is a statistically significant negative association between education and Net-confidence: more educated people tend to be more sceptical of the information and people in cyberspace and the institutions of the Internet than individuals with less schooling. Also, those with higher

educational qualifications are less concerned over Net-risks (see Tables 3 and 4).

This indicates that education and exposure to the Internet might offer a general strategy for coping with the actual risks and perceived threats relating to the trustworthiness of the network and the global virtual world of resources and services to which it gives access. However, since education and exposure to the Internet and ICTs are skewed towards higher socio-economic groups, these strategies could reinforce the 'digital divide' in access to the Internet over time. This threat is somewhat diminished by the way the Internet is becoming so widely accessible in Britain, but advances such as broadband Internet will continue to raise issues of the digital divide in access and trust (Dutton *et al.* 2003).

The Internet as an experience technology

The most general association is between Internet use and trust, measured by the two dimensions of Net-confidence and Net-risk. Those exposed to the Internet gain more trust in the technology (Tables 1 and 2). Even past users, the so-called 'Internet dropouts', have more confidence in the Internet than do non-users who have no experience with the technology (Tables 1 and 2). Most predispositions to cybertrust that are associated with social and demographic characteristics tend to be mitigated over time and can be accounted for by the lessons learned from experience online (Tables 3 and 4). Most generally, the analysis indicates that levels of cybertrust (confidence and risk) are related to an individual's patterns of use or non-use of the Internet over time, which supports the view that the Internet is an 'experience technology'.

Users of the Internet have more certainty and more confidence in the information and people they can access through the technology than do non-users, with many non-users having no opinion about its trustworthiness. At the same time, the more experienced users are more likely to encounter, and therefore be aware of, bad online experiences. This suggests that initiatives to enhance the trustworthiness of the Internet are warranted. However, these efforts are likely to create a tension by competing against other values, such as privacy or access, which could be threatened by some trust-enhancing services (Guerra *et al.* 2003).

The concept of a certainty trough helped the study team to explore the influence of proximity to the Internet as a factor shaping cybertrust, but the findings are not entirely consistent with an explanation based on MacKenzie's conception of this phenomenon. First, those who have rejected the Internet are more certain and more trusting than those with no experience of the Internet, which suggests that 'social proximity', or experience, might be a more straightforward explanation of low certainty than alienation or a

rejection of the technology. Second, we found no clear rise of uncertainty among the most experienced users, except as it might be connected with bad experiences online.

As these findings may have arisen because we had not looked closely enough at actual producers, who are those most proximate to the technology, we developed a combined indicator of Internet confidence and risk across three 'categories of proximity': 'non-users'; users who have never produced their own website (whom we called 'consumers'); and users who have created their own site ('producers'). Analysing attitudes to Internet confidence and Internet risk, across these categories (Figure 3), shows that producers have slightly more confidence than Internet users. This is a minor exception to the pattern expected by a certainty trough, but consistent with an experience technology. There is no evidence of a trough when it comes to concern about Internet risks, although there is clear indication of a decline in concern the more proximate the person is to the Internet, with producers generally significantly less concerned about any associated risk.

Thus, within the range of respondents surveyed, there is more evidence for the Internet as an experience technology – with proximity promoting more cybertrust – than for a curvilinear certainty trough. There might be a diminishing level of trust or greater uncertainty at the highest end of expert producers, such as in the case of computer scientists. However, that was not the case in this more representative cross-sectional sample in the OxIS study.

Bad experiences

The longer a person uses the Internet, the more likely he/she is to have experienced one or more problems when online. We asked users whether

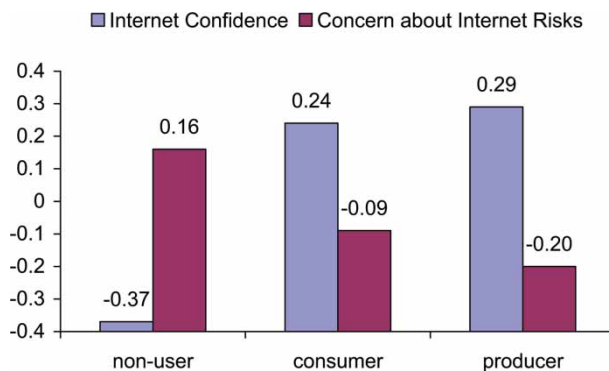


FIGURE 3 Trust by Internet non-users, consumers and producers ($n = 2029$) (average factor scores for each dimension of cyber trust: confidence and risk).

they had problems with some of the negative Internet experiences that are frequently mentioned (Figure 4). The most frequently experienced negative online experience reported (at 23 per cent) was of obscene or abusive email. Receiving a computer virus, being contacted by someone from a foreign country suggesting a fraudulent arrangement to make money or receiving mail intended for someone else were the next most common experiences. A worrisome but relatively small percentage of users indicated other problems such as excessive online bills.

There has been much news coverage of the kinds of bad online experience represented in Figure 4, which makes these figures surprising in many respects. For example, less than 1 per cent of email users said that their credit card details were stolen by someone over the Internet, although this was one of the major initial cybertrust fears. The bad experiences are also generally at a lower level than many have expected, with just over half of users saying they did not experience any of the problems listed.

In weighing up this finding, it should be remembered that many use the Internet in a far more limited way than the heaviest users, such as in academe and the computer industry. At the same time, those who use the Internet more might be a bell-wether for the problems likely to beset others in due course. The relatively limited encountering of bad Internet experiences found in this study is therefore not a reason for complacency. Moreover, ‘bad Internet experiences’ are negatively related to Net-confidence (see Table 3) and positively associated with perceived Net-risks (see Table 4),

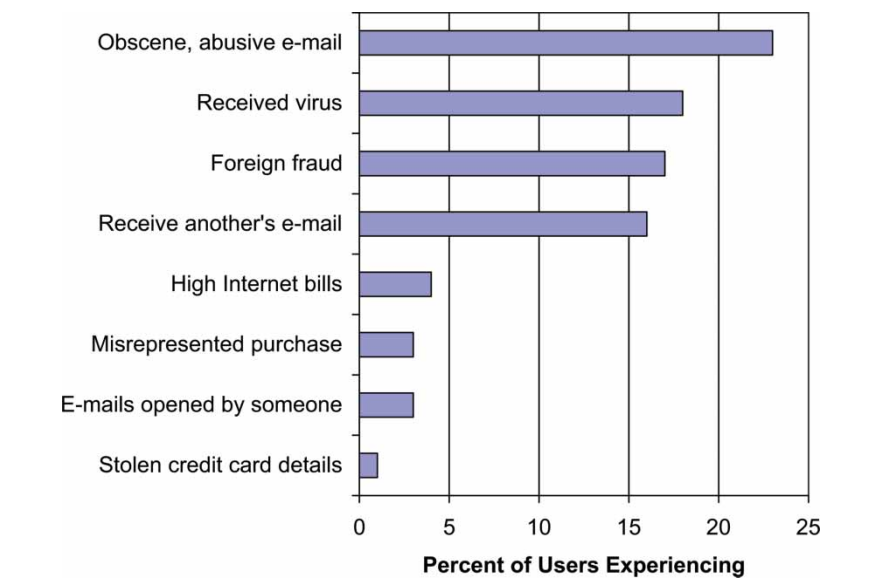


FIGURE 4 Bad experiences on the Internet (*n* = 1045).

indicating that bad experience does undermine trust, creating a countervailing influence for experience online.

The impact of trust on Internet use

Does trust matter in the subsequent use of the Internet? As reported above, Internet dropouts perceived somewhat greater risks in the use of the Internet. This suggests that distrust might help explain why some people stop using the Internet. The relationships found between use of the Internet generally and levels of Net-confidence and Net-risk are also likely to be, in part, two-directional. That is, use could engender trust, but trust could reinforce decisions to get online.

There is therefore some evidence to support the commonsense view that trust is an important factor in the future of the Internet. To explore the degree to which trust is related to the use of the Internet for online shopping, one use of the Internet that has been associated with experience and trust, OxiS respondents who use email were asked to indicate the approximate number of online purchases they made per month. In line with findings in the US, the strongest relationship is with proximity to the Internet (Lunn & Suman 2002): those more likely to shop online are also generally those who have used the Internet for more years for more types of activities and have a higher level of expertise in the technology or its use (Table 5). Those with more Net-confidence are somewhat more likely to shop online, but this relationship is not statistically significant. However, perceived Net-risks are significantly and negatively associated with online shopping. In short, as many suspect, it appears that distrust of the Internet undermines e-commerce.

TABLE 5 Regression for 'online shopping' among users ($n = 1045$)^a

<i>variable</i>	<i>B*</i>	<i>std. error*</i>	<i>beta**</i>	<i>t</i>	<i>sig.</i>
constant	-0.14	0.39		-0.37	0.71
gender (female)	0.25	0.21	0.04	1.17	0.24
SES	0.13	0.08	0.06	1.75	0.08
age	0.01	0.00	0.04	1.32	0.19
education	0.10	0.06	0.06	1.76	0.08
broadband	0.30	0.20	0.05	1.47	0.14
proximity	0.42	0.08	0.16	4.87	0.00
net-confidence	0.09	0.08	0.03	1.07	0.29
net-risks	-0.25	0.07	-0.10	-3.38	0.00

^aOnline shopping measured by number of purchases per month; *Unstandardized coefficients; **Standardized coefficients.

Thus, two countervailing trends seem to be shaping the future of e-commerce and, quite probably, other online services. As people get closer to the Internet, they tend to gain, or learn, an educated level of cyber-trust. However, with experience can come bad experiences with such problems as viruses, spam and obscene mail. This tends to increase a sense of the risks entailed in the use of the Internet, which can undermine trust and use of the technology.

Value and limits of survey research on cybertrust

A developing literature on trust and risk associated with ICTs is most often anchored in case studies and ethnographic approaches, which highlight the subtle but no less real complexities of expert and public perceptions. Survey research can complement these studies in a variety of ways because it is one of the few means available to provide an indication of patterns and trends across a large population, like that of Great Britain. Also, by enabling multivariate statistical controls, survey data permit the exploration of underlying patterns in a manner that would not be possible with small samples and qualitative observations.

In allowing for generalization to a wider population, survey research can also identify explanations that could evade case research, such as the significance of experience to perceptions of cybertrust that emerged from the OxIS study through the making of comparisons across many users at different stages of involvement. Commonly held assumptions can also be countered by surveys, such as this study's failure to support some conventional explanations of public perceptions as being tied to particular social groups. Likewise, the certainty trough did not provide a valid interpretation of our findings, although it led us towards an alternative explanation, more consistent with the results – the concept of an experience technology.

Despite survey research's analytical advantages and ability to project to a larger population, this methodology has limitations, particularly in cross-sectional surveys. For instance, the study reported here highlights issues concerning cybertrust for which more evidence and analysis is needed to gain a better understanding of the underlying social dynamics. Surveys are also generally weak in providing detailed contextual knowledge and in unravelling the full complexity of individual beliefs, motivations and actions. Therefore, these analyses could be complemented by more qualitative research.

The OxIS survey reported here is also a snapshot at one point in time.¹¹ Longitudinal surveys would enable stronger conclusions to be drawn regarding any causal relationships suggested by the associations identified in this paper, particularly given the degree to which trust appears to be anchored in experiences online. Will more users have more frequent negative

experiences online, or will contemporary problems, such as spam, diminish as they are taken more seriously and anticipated?

These limitations are mitigated to some extent by a degree of replication across surveys, some of which have relied on longitudinal data. For example, the findings of this survey analysis generally reinforce those of Lunn and Shuman's (2002) longitudinal study in the US. Studies within the World Internet Project (WIP) hold out the potential for further replication across nations and over time.¹²

Digital divides and other social issues of a 'trust tension'

The OxlS findings about the ways in which social distance and know-how relate to social inequities suggest that cybertrust might reinforce the digital divide in the use of ICTs. People with the appropriate skills and resources to get online, and the educational background to collate and interpret online information, could enhance their ability to authenticate the value of products, services and information, thereby protecting themselves against cyber fraud and crime. However, others with less expertise tend to remain offline, fail to experience the Internet and are more likely to distrust the technology.

The value to e-business and e-government of finding effective means of establishing identity and trustworthiness to overcome these fears has stimulated the development and application of many privacy-enhancing tools and services (Guerra *et al.* 2003), as well as interest in privacy regulations (e.g. OECD 2002) and cybercrime legislation (e.g. US CAN-SPAM [Controlling the Assault of Non-Solicited Pornography and Marketing] Act of 2003). To the degree that these initiatives are effective in diminishing bad experiences online, they might help shore levels of cybertrust.

However, these methods confront a 'trust tension' (Guerra *et al.* 2003) between privacy concerns and the need to gather data to help confirm e-identities. Finding an appropriate framework to address this tension, by balancing consumer protection with the need for a free flow of traffic on e-networks, involves many interrelated uncertainties: economic, psychological, institutional, technical and legal. Unravelling and gaining a better understanding of these requires social research with a broad perception of the co-evolutionary nature of human, organizational and technological systems, such as the way the Internet and related ICTs 'reconfigure access' to information, people, services and technologies (Dutton 1999; Dutton *et al.* 2003).

Summary: the Internet as an experience technology

The study reported here illuminates the view that the Internet can be called an 'experience' technology, as it is difficult for people to understand how the

Internet and Web work until they use them. This could provide a better interpretation of the social dynamics of cybertrust than explanations anchored in categories of users, such as suggested by literature on risk cultures (Douglas & Wildavsky 1982). Proximity variables and levels of use, such as indicated by broadband use, were consistently significant in all the analyses but demographic variables relating to cultural settings were not. While social network and cultural settings might help account for differences in attitudes among non-users, such as across age groups, this does not help interpret findings across categories of users as strongly as the influence of experience on perceptions of cybertrust.

Non-users are generally more distrustful of the Internet. They have less confidence in information and people online, and in the institutions 'running' the Internet. They are also more concerned about the potential risks. Distant from the technology, they are most uncertain of its value. The risks experienced in using the Internet are most often less than the risks imagined by non-users, who also often underestimate the benefits of the Internet.

On the other hand, as people use the Internet more they gain greater expertise and capabilities for accessing Internet resources. They are then likely to be less concerned over the risks of Internet use, although they are aware of risks attached to such use. Time and involvement with the Internet bring some bad as well as good experiences, which can both undermine and boost confidence in the technology. Before problems with Internet use grow, as use is taken up more widely for more activities, the relatively low level of bad experiences found in the study might suggest that it is timely to undertake initiatives to reduce the risk of more users experiencing greater difficulties.

A closely related pattern is the degree to which there is lower trust of the technology among categories of users, such as the less affluent, who have less access to the Internet. It is within these groups that real experience in using the Internet has a particularly disproportionate positive impact, increasing their trust in the Internet and lessening their preconceived concerns over risks.

Notes

- 1 A discussion of Internet adoption is provided by Rose (2003); also see Dutton *et al.* (2005); and recent results of the World Internet Project at <http://www.worldinternetproject.net> (accessed 27 June 2006)
- 2 A comprehensive overview of research on the factors related to the perception of risk generally is provided by Jackson *et al.* (2003).
- 3 Limited space in this paper allows for only a summary of the analysis on cybertrust undertaken on data from the OxIS 2003 interviews. Fuller details are provided in Dutton and Shepherd (2003, 2005).

- 4 For a more detailed description of the sampling method, see Dutton and Shepherd (2003, Appendix 7.1), which is available online.
- 5 The OxIS questionnaire and additional information about the survey are available online at: <http://www.oii.ox.ac.uk/research/project.cfm?id=8> (accessed 27 June 2006).
- 6 Questions on information reliability also related to newspaper and television. The question on institutional influences mentioned, in addition to the Internet: major companies; the Government; television news; and newspapers. Although it is arguable that nobody 'runs' the Internet in the same way people run, say, newspapers or television, pre-tests and experience during the interviews did not surface confusion on this issue. Confidence in the people communicated with on the Internet was compared with confidence in: scientists; doctors; 'most people I know'; and 'most people in this country'.
- 7 The factor analysis is described in detail in Dutton and Shepherd (2003, Appendix 7.2), and is available online.
- 8 The exact operational definition is provided, along with the underlying factor analysis, in Dutton and Shepherd (2003, Appendix 2), which is available online.
- 9 Ordinary least squares regression analysis was used to develop the findings reported in this paper. It is the best understood type of regression and appropriate to this study as the dependent variable was continuous. The two independent variables chosen were: demographic and experience. The literature shows that demographic characteristics, such as age and gender, have an impact on Internet use. The experience variable addresses the certainty trough concept by capturing respondents' interaction with the Internet, both currently and in the past.
- 10 Socioeconomic status was captured by the standard British social profile.
- 11 A further OxIS survey that asked similar questions on cybertrust was conducted in 2005 (see <http://www.oii.ox.ac.uk/research/project.cfm?id=8>).
- 12 WIP reports include one by UCLA's Center for Communication Policy (CCP 2003). See <http://www.worldinternetproject.net> (accessed 27 June 2006) for information about WIP centres and reports.

References

- Ben-Ner, A. & Putterman, L. (2002) *Trust in the New Economy*, HRRI Working Paper 11-02, University of Minnesota, Industrial Relations Centre, Minnesota.
- CCP (2003) Center for Communication Policy, *The UCLA Internet Report: Surveying the Digital Future: Year Three*, UCLA Center for Communication Policy, Los Angeles, CA. [Online] Available at: <http://ccp.ucla.edu/pdf/UCLA-Internet-Report-Year-Three.pdf>
- Douglas, M. & Wildavsky, A. (1982) *Risk and Culture: An Essay on the Selection of Technical and Environmental Dangers*, UC Press, Berkeley, CA.

- Dutton, W. H. (1999) *Society on the Line: Information Politics in the Digital Age*, Oxford University Press, Oxford.
- Dutton, W. H. (2004) *Social Transformation in the Information Society*, UNESCO Publications for the WSIS, Paris.
- Dutton, W. H. & Shepherd, A. (2003) *Trust in the Internet: The Social Dynamics of an Experience Technology*, OII Research Report No. 3, Oxford Internet Institute, Oxford, University of Oxford. [Online] Available at: <http://www.oii.ox.ac.uk/research/publications.cfm> (27 June 2006).
- Dutton, W. H. & Shepherd, A. (2005), 'Confidence and risk on the Internet', in *Trust and Crime in Information Societies*, eds R. Mansell & B. S. Collins, Edward Elgar, Cheltenham, pp. 207–244.
- Dutton, W. H., di Gennaro, C. & Hargrave, A. M. (2005) *The Internet in Britain: The Oxford Internet Survey (OxIS)*, OII, University of Oxford, Oxford, May.
- Dutton, W. H., Gillett, S. E., McKnight, L. W. & Peltu, M. (2003) *Broadband Internet: The Power to Reconfigure Access*, Forum Discussion Paper No. 1, Oxford Internet Institute, Oxford. [Online] Available at: <http://www.oii.ox.ac.uk/research/publications.cfm> (27 June 2006).
- Flanigan, A. & Metzger, M. (2000) 'Perceptions of Internet information credibility', *Journalism & Mass Communication Quarterly*, vol. 77, no. 3, pp. 515–540.
- Giddens, A. (1990) *The Consequences of Modernity*, Stanford University Press, Stanford, CA.
- Guerra, G. A., Zizzo, D. J., Dutton, W. H. & Peltu, M. (2003) Economics of Trust: Trust and the Information Economy, DSTI/ICCP/IE/REG(2002)2 (Paris: OECD). Also available as Guerra, G. A., Zizzo, D. J., Dutton, W. H. & Peltu, M. (2003), *Economics of Trust in the Information Economy*, OII Research Report No. 1, Oxford Internet Institute, University of Oxford, Oxford. [Online] Available at: <http://www.oii.ox.ac.uk/research/publications.cfm> (27 June 2006).
- Jackson, J., Allum, N. & Gaskell, G. (2003), *Public Perception of Risk: A Review of the Research Literature*, Methodology Unit, London School of Economics and Political Science, London, November.
- Katz, J. & Rice, R. E. (2002) *Social Consequences of Internet Use: Access, Involvement, and Interaction*, MIT Press, Cambridge, MA.
- Lohse, G. L., Bellman, S. & Johnston, E. J. (2000) 'Consumer buying behavior on the Internet: findings from panel data', *Journal of Interactive Marketing*, vol. 14, pp. 15–29.
- Lunn, R. J. & Suman, M. W. (2002) 'Experience and trust in online shopping', in *The Internet in Everyday Life*, eds B. Wellman & C. Haythornthwaite, Blackwell, Oxford, pp. 549–577.
- MacKenzie, D. (1999) 'The certainty trough', in *Society on the Line*, ed. W. H. Dutton, Oxford University Press, Oxford, pp. 43–46.
- OECD (2002) *Guidelines on the Protection of Privacy and Transborder Flows of Personal Data*, OECD, Paris.

- Riegelsberger, J., Sasse, M. A. & McCarthy, J. D. (2003) 'The researcher's dilemma: evaluating trust in computer-mediated communication', *International Journal of Human-Computer Studies*, 58, pp. 759–781.
- Rose, R. (2003) 'The dynamics of digital choice', paper delivered at the Information, Communication, Society Symposium, Oxford Internet Institute, University of Oxford, 19 September.
- Short, J., Williams, E. & Christie, B. (1976) *The Social Psychology of Telecommunications*, Wiley, London.
- Urban, G. L. & Sultan, F. (2000) 'Placing trust at the center of your Internet strategy', *Sloan Management Review*, vol. 42, no. 1, pp. 39–48.
- Uslaner, E. (2000) 'Trust, civic engagement and the Internet', paper presented at the Joint Sessions of the European Consortium for Political Research, University of Grenoble, Switzerland, April.
- Wallace, P. (2001) *The Psychology of the Internet*, Cambridge University Press, Cambridge.

William Dutton is Professor of Internet Studies at the University of Oxford where he is Director of the Oxford Internet Institute and a Fellow at Balliol College. He has published widely on the social and political dynamics of information and communication technologies. Recent books include *Society on the Line* (Oxford University Press, 1999), *Digital Academe*, edited with Brian D. Loader (Taylor & Francis Routledge, 2003), *Social Transformation in the Information Society* (Paris: UNESCO Series for the WSIS, 2004) and *Transforming Enterprise*, edited by Dutton, Brian Kahin, Ramon O'Callaghan and Andrew W. Wyckoff (MIT Press, 2005). Address: Director, Oxford Internet Institute, University of Oxford, 1 St Giles', Oxford OX1 3JS, UK. Tel: +44 (0)1865 287210; Fax: +44 (0)1865 287211. [email: William.Dutton@oii.ox.ac.uk]

Adrian Shepherd is on the staff of the Research, Development and Statistics Directorate of the Home Office. Prior to joining the Home Office, Dr Shepherd was the survey research officer at the Oxford Internet Institute, where he worked on the analysis of the 2003 Oxford Internet Survey (OxIS). Address: Home Office, Direct Communications Unit, 2 Marsham Street, London SW1P 4DF, UK. Tel: +44 (0)20 7035 4848. [email: Adrian.Shepherd@ons.gsi.gov.uk]
